REMARKS/ARGUMENTS

The NPL Unreadable Document

The Examiner indicates that the NPL document TCPA PC Specific Implementation Specification is unreadable. That document is unfortunately difficult to read. The applicant recently filed another IDS with a document, which we understand has basically the same disclosure as the difficult to read document, but document which should be fair easier to read.

The Objections to the Claims

The Examiner objected to a number of claims. Since claims 1 - 34 are cancelled, without prejudice, by this response, the 'a' versus 'an' issue does not need to be addressed. With respect to the 'authorisation' versus 'authorization' issue, the applicant has made the requested amendment to the claims, but points out that 'authorisation' is not a mis-spelling, rather it is an alternative spelling of 'authorization' which alternative spelling is more commonly used in the British Isles than in the US, but, even so, the MPEP makes it clear that the use of British English is quite proper in a US patent application. See MPEP 608.01. So while the amendment has been made, there is nothing wrong with using British English spellings in US patent applications.

The Prior Art Based Rejections

The Examiner rejected all of the pending claims on prior art grounds. As noted above, claims 1 - 34 have been cancelled without prejudice and claim 35 has been amended to recite:

> a memory for storing a current decryption-root key;
> a decrypted-access arrangement arranged to restrict decrypted access to the hierarchy nodes to those nodes

> decryptable by a chain of decryption rooted in said current decryption-root key; and
>
> a current-decryption-root setting arrangement for storing in said memory, in decrypted form, the key of a selected non-leaf node of said hierarchy to serve as said current decryption-root key, the current-decryption-root setting arrangement enabling the selected non-leaf node to be changed.

The first two elements are fairly standard (the nature of the hierarchy is such that decrypted access to a node necessarily involves a chain of decryption passing down the hierarchy – in the case of the prior art, starting with the storage root key). The third element (in combination with the other elements) provides the inventive aspect recited by claim 35, that is, the ability to change the effective root of the chain of decryption.

The Prior Art References

On page 3 of the official action, the Examiner rejects original claim 35 as being obvious in view of Matayas (US 4.941,176) and Challener (US 2002/0059256).

Claim 35, as presently amended, specifies that the non leaf nodes of the hierarchy "each comprise, in encrypted form, a key used to encrypt the or each of its child nodes". This is not disclosed in Matayas, where the keys are stored encrypted under a key formed by a combination of a control vector and a master key; although there are special key-encrypting keys, KEKs, these are stored in their own hierarchy (see Figure 7, again each of these keys is encrypted for storage using a key formed by a combination of a control vector and a master key) and the KEKs are only used to encrypt keys for transmission, not storage. See col 9, line 57 to col. 10, line 10 of Matayas.

On page 7 of the Official Action at item 10, the Examiner asserts that Matayas does disclose a key hierarchy with parent keys being used to encrypt

their child keys. However, the passages referred to do not disclose this. The referenced passages are all concerned with key generation (see col. 8, lines 23-28). The basic operation is as described at col. 8, lines 32 to 38:

> "The cryptographic processing unit 16 then operates in response to the authorization signal on line 20 to output the random number as a first generated key in encrypted form in which the random number is encrypted in a key which is the logical product of the first associated control vector C3 and a first key K1."

There is no reference to any hierarchy though, of course, it one might assert that having one key encrypted by another key provides a two-level hierarchy. However, claim 35 requires there are multiple non-leaf nodes which in turn requires at least three levels to the hierarchy (a two-level hierarchy only has a single non-leaf node: the root node).

However, this point is somewhat academic as Challener relates to the same type of protected storage hierarchy as the present application and has a node hierarchy in which the non-leaf nodes each comprise a key used to encrypt the or each of its child nodes This actually is not well described in Challener though a skilled reader would understand this and paragraph 0021 of Challener does provide a brief description.

An important point to appreciate at this stage is the difference between a migratable key and a non-migratable key – these terms are used in paragraph 0021 of Challenger but do not appear to be explained (probably because the TCPA specification, incorporated by reference, does this). Anyway an explanation is given at lines 10-12 on page 2 of the present application. A migratable key can be exported from a TPM.

What the examiner appears to be arguing in the second paragraph on page 6 of the Official Action is that the indicated passage of Challener, i.e.:

> "Thus, migrating this key to a new platform also effectively migrates all the keys below it. The user key 103 is a migratable private 2048 RSA key wrapped by the platform key 102 and used as a root for all the user's migratable keys."

discloses changing the node of the hierarchy serving as the current root node. This is clearly wrong. What the quoted passage effectively teaches is that a sub-hierarchy of the original hierarchy can be moved to a new platform (this can only be done where the key at the head of the sub-hierarchy is a migratable key). However, this says nothing about the effective root key of the original hierarchy on the original platform – these remain unchanged. So, with all due respect, the Examiner's argument fails.

Claim 35 as now presented, makes it clear that decrypted access to a node is only possible if the node can be decrypted by a chain of decryption rooted in a current "decryption-root" key where the key serving as the decryption-root key can be changed between keys of non-leaf nodes of the hierarchy – all this being in respect of the same hierarchy. The term "decryption-root key" is newly introduced for the purpose of avoiding the confusion apparently caused by the original term "current root key"; the hierarchy has only one root (the "storage root key" of the described embodiment) but the key serving as the root of the chain of decryption needed for decrypted access to a node can be changed, effectively changing what nodes can be decrypted. This is not disclosed in either Matayas or Challaner.

Statements of Invention

The former statements of invention set forth at paragraphs 0011-0021 have been amended to better relate to the subject matter of the present claims.